Zoom issues - update

Threat Alert 20-015 - Date: 30/04/2020 - Version: 1.0

TLP:GREEN

FOR ACTION	Category	Type	Threat Level	Domain	Sector	Confidence
	Cybercrime Cyberespionage	Privacy leaks	Medium	World	Digital services, videoconferencing	A1

Key Points

- Since CERT-EU's initial Threat Alert TA-20-014 on Zoom security and privacy issues, released on 6 April 2020, a number of updates have mitigated or reduced some of the problems that were highlighted.
- Some Zoom risks can also be curtailed by better user awareness.
- Zoom's weak encryption, one of the main issues that made us strongly discourage Zoom use in EU institutions, bodies and agencies (EU-I), has been purportedly fixed in version 5. However, this should be checked and tested.
- Ties with China remain an important issue when evaluating Zoom use in EU-I. A transparency report would hopefully shed some light on these ties.
- At this stage, CERT-EU considers Zoom a suitable videoconferencing platform for EU-I's public and semi-public events such as leisure or training and education with non-sensitive material. However, using Zoom to conduct EU-I sensitive meetings is not recommended.

Summary

On April 6, CERT-EU issued Threat Alert TA-20-014 regarding security and privacy issues in the Zoom videoconferencing platform. The software, which use has been significantly growing in the wake of the COVID-19 crisis, allows for easy digital collaboration through video chat, screen sharing, and breakout sessions. The boom in its usage has also attracted heightened attention from security researchers.

Since CERT-EU's initial Threat Alert was released, Zoom has issued updates and blog posts resolving and explaining some of the issues that were brought forward by the security community and reported on by CERT-EU. Annex I contains a list of the issues mentioned in TA-20-014, as well as other problems that have since come to light. The number of issues is not necessarily an appropriate gauge of the security situation of the platform, as they do not all have the same level of severity.

The issues and associated changes made by Zoom fall into 4 categories.

Vulnerabilities and Patching

Some of the issues with the Zoom platform were solved through patches. The first set, on March 28, removed the Facebook software development kit (SDK) in the iOS app, which sent personal data from the user to Facebook even if the user did not have an account there. This resolved issue #9 in the Annex.

The second set of patches, issued on April 2 and mentioned in TA-20-014, addressed two vulnerabilities in macOS. Those were the UNC (Universal Naming Convention) credential stealing issue, and the Attention Tracking feature that raised privacy concerns. This set resolved issues #10, #11, #13 and #15 in the Annex.

The third set of patches, released on April 8, removed the Zoom ID from the meeting window after some users posted screenshots of their meetings on social media, revealing their IDs and causing questions about user prudence. Although some of the postings did constitute a security risk (such as the UK Prime Minister posting the Cabinet meeting ID), some others had a limited impact (such as most of Parliament Committee meetings in Belgium, which are public records). Zoom also patched the Waiting Room vulnerability mentioned in the Annex. This last update resolved issues #6, #14 and #17 in the Annex.

Issue #18, zero-days for Zoom software being sold, is difficult for Zoom to mitigate as the buyer of this kind of information will likely not disclose it to Zoom. All software suffers from zero-day vulnerabilities[1], and there is not enough information at this point to state that Zoom will be more susceptible to exploitation than other platforms.

Cisco Talos discovered[2] a cloud-side Zoom vulnerability that could allow arbitrary users to request contact lists of arbitrary registration domains (issue #19 in the table). In the reply, the Zoom server disclosed a directory of users registered under

[1] https://zerodium.com/program.html

[2] https://blog.talosintelligence.com/2020/04/zoom-user-enumeration.html

this domain. This would allow attackers to send the users spear-phishing messages and socially engineer them into installing malware, possibly masqueraded as an update to the Zoom client. The vulnerability appears to be patched now.

User education

Zoom has published many blog posts detailing how to set up meetings securely, use passwords and waiting rooms, lock meetings after everyone has joined, share meeting links, use the Personal Meeting ID (PMI), etc. This has been a great help for users not too familiar with the platform. Issues #8 and #16 will be mitigated with these information sessions. Also, Zoom has enforced passwords by default for meetings. This alleviates the risks associated with issue #8 (Zoombombing), making intrusions much more difficult.

Zoom's efforts in educating users are also reflected in issue #7: fake or malicious Zoom domains. These typosquatting and domain mimicking attacks are not new and certainly not limited to Zoom. Any web-based platform can suffer from these attacks and it is almost impossible for Zoom to resolve this through technical means. Users should be made aware how to distinguish real from fake domains.

Policy changes

Zoom has introduced some policy changes that they state will improve the security posture of the platform. In a 90-day plan revealed on April 1, a number of measures were announced, such as focusing development effort on security and privacy rather than features, preparing a transparency report, launching a CISO council, etc. One result of these policy changes appears to be the Data Routing feature that was released on April 18, which gives paying users limited control over which geographical regions their data passes through.

In Zoom version 5, meeting hosts and co-hosts can report a user in their meeting who is misusing the Zoom platform. The complaint will go to Zoom's Trust & Safety team, who will "review any potential misuse of the platform and take appropriate action".

Zoom has been highly responsive to community criticism about its security and privacy issues. And while many vendors would start a public relations campaign to improve its reputation, Zoom has also made real and substantial efforts towards resolving some of the problems raised by researchers.

Some security researchers have come out in support[3] of Zoom[4], especially after mainstream media picked up on the Zoom security and privacy issues. Whilst some news outlets have provided research reports without context thus likely blowing certain issues out of proportion, however, the fact remains that some issues are serious. The number of vendors drawing on China for development does not discount the fact that Chinese cybersecurity law allows for any entity in China to be coerced into collaborating with security services (see Annex, item 5).

Encryption and privacy

Encryption mode (issue #1). With the announcement[5] of version 5, available from April 27, Zoom introduced AES 256-bit GCM stream cipher encryption. This is much better suited for a video conferencing platform than the previously used block cipher. According to Zoom, it "provides more protection for meeting data and greater resistance to tampering". However, while it almost certainly provides better security for data in mid-transit, it does not provide full end-to-end encryption. This is not unusual as almost no teleconferencing solutions manage to provide full end-to-end encryption simultaneously to a large number of participants.

Single shared key (issue #2). In their testing, Citizen Lab found that a single AES-128 key was used in ECB mode by all meeting participants to encrypt and decrypt audio and video. Since, on April 27, Zoom introduced a new encryption mode in version 5 (see issue #1 above). CERT-EU has received information from the company indicating that participants will continue to share a common key but that it will be a 256 bits key used in GSM mode as indicated above.

Encryption key generated by Zoom servers (issue #3). In their testing, Citizen Lab also found that the keys appeared to be generated by Zoom servers. CERT-EU has received information indicating that a Key Management System (KMS) on a MultiMedia Router (MMR) generates the shared symmetric encryption key for the specific session using a "cryptographically secure random number generator", holds it in memory, and transmits it to the client. As indicated above, each client receives the same key. As each additional participant joins, the KMS provides the specific session key to the respective client through the meeting server they use to connect. The key is treated as need-to-know and not shared beyond the clients and servers within a given session. Upon ending the meeting, the shared encryption key for the specified session will be purged from the memory of the MMR and the clients.

Comments

CERT-EU has taken into consideration the material that has been published both by Zoom and by security researchers since its Threat Alert of April 6. Zoom has demonstrated commitment to improved security. Many shortcomings outlined

[3] https://medium.com/@vince_17729/zooming-to-conclusions-20560d9f40b9
[4] https://www.linkedin.com/pulse/strange-zoom-pile-on-robert-walker/
[5] https://blog.zoom.us/wordpress/2020/04/27/its-here-5-things-to-know-about-zoom-5-0/

by security researchers have been addressed and others are on the way of being addressed. With the introduction of AES 256-bit GCM encryption in version 5.0 and geocontrols for data transit, Zoom is taking steps in the right direction.

CERT-EU considers Zoom a suitable videoconferencing platform for training, education and leisure use. However, Zoom's significant ties with China and limited transparency remain significant issues. Therefore, using Zoom to conduct EU-I sensitive meetings is not recommended.

CERT-EU will continue monitoring the situation and will review its recommendations as necessary.

Annex I – Overview of recent security and privacy issues, not in order of severity

Nr.	Issue	Description	Status	Comment
1	Weak encryption	Audio and video streams use AES128 ECB encryption.	Solved in Zoom 5.0	New 256-bit GCM encryption, to be checked and tested.
2	Single shared key	All participants use the same encryption key, even after they have left the meeting.		No change on this specific issue. Testing the new encryption mode would be necessary.
3	Encryption key generated by Zoom servers	The meeting encryption key is generated by Zoom servers and distributed to participants rather than participants generating keys.		No change on this specific issue. Testing the new encryption mode would be necessary.
4	Some meetings routed through China	Some Zoom meetings saw its traffic routed through or managed on Chinese servers. This raises privacy issues.	18-04-2020 Control over routing	Zoom gives users some geographical control over data routing.
5	Chinese ties	Zoom has allegedly 700 employees in China for development of its software. Chinese cybersecurity law allows for blanket seizure of data. See TM-190423-1 and TM-191209-1.		Will likely not be resolved.
6	Waiting Room vulnerability	Citizen Lab researchers uncovered what they called a severe vulnerability in Zoom's Waiting Room feature. No details public.	08-04-2020 Resolved	Unknown – in Responsible Disclosure process.
7	Fake or malicious Zoom domains	Cybercriminals have registered fake Zoom domains tricking users to download malware.	Zoom cannot solve this	All popular platforms will suffer from this issue.
8	Zoombombing	Disruption of unsecured Zoom sessions.	05-04-2020 Zoom enforced passwords by default	Users should follow Zoom's guidelines.
9	iOS privacy breaches	Facebook module in iOS Zoom app sent user data to Facebook, even if that user did not have a Facebook account.	28-03-2020 Removal of Facebook SDK	
10	macOS privilege escalation	Vulnerability in Zoom's macOS client allowed for privilege escalation.	02-04-2020 Patched	
11	macOS vulnerability	Vulnerability in Zoom's macOS client allowed unauthorised microphone, camera and meeting recording activation.	02-04-2020 Patched	
12	Misleading macOS installer	Misleading system prompt to expedite installation.	Not a vulnerability	Bad coding practice.
13	Windows credential theft	UNC vulnerability allowed for stealing of Windows credentials if a malicious link was clicked in the chat.	02-04-2020 Patched	
14	Unwarranted calls and info leaks	Zoom users from the same e-mail domain were able to call each other	08-04-2020 Removed	
15	Attention tracking	The Attention Tracking feature allowed for the meeting host to see who had the meeting in focus.	02-04-2020 Removed	
16	Zoom Personal Meeting ID (PMI) is a permanent meeting	Using this PMI instead of generating one for each meeting can lead to unwanted Zoom sessions.	Users are partly responsible	As of 5 April, 2020, all meetings require a password by default. However, careless users may still public post invitation links, which contain passwords.
17	Users posting photos of Zoom sessions revealed meeting ID	Some users post photos of their Zoom sessions on social media. This would leak the meeting ID.	08-04-2020 ID removed from window	Users are partly responsible.
18	2 zero-days for Zoom clients	Hackers are selling 2 zero-day vulnerabilities for Zoom clients on macOS and Windows.	Hard for Zoom to mitigate	All platforms suffer from this.
19	Zoom user enumeration	A malicious user can obtain a complete list of Zoom users inside a specific organisation.	21-04-2020 Patched	Cloud-side vulnerability, users do not have to apply a patch.

	Resolved
	To be checked and tested
	Not resolved
	Not applicable
	Unknown